Three-Level Password Approach in Granting User Access to Shared Folders

Syarifah Bahiyah Rahayu[1,2]
[1]Cyber Security and Digital Industrial Revolution Centre
[2] Dept. of Defence Science, Fac. of Def. Science & Tech.
National Defence University of Malaysia
5700 Kuala Lumpur, Malaysia
syarifahbahiyah@upnm.edu.my

Iqbal Shamsudheen
Department of Defence Science
Faculty of Defence Science & Technology
National Defence University of Malaysia
57000 Kuala Lumpur, Malaysia
iqbal@upnm.edu.my

Mohd Sidek Fadhil Mohd Yunus
Department of Defence Science,
Faculty of Defence Science & Technology
National Defence University of Malaysia,
57000 Kuala Lumpur, Malaysia
sidek@upnm.edu.my

Mohd Hazali Mohamed Halip[1,2]
[1]Cyber Security and Digital Industrial Revolution Centre,
[2]Dept of Comp. Science, Fac. of Def. Science & Tech.
National Defence University of Malaysia,
57000 Kuala Lumpur, Malaysia
hazali@upnm.edu.my

Abstract — **An established file sharing infrastructure can be a huge convenience for organizations to allow members of all levels within an organization to collaborate and share data. While allowing multiple access to files and folders, the privacy and secrecy of files that reside in the shared space become something of a tradeoff among users. It has now become a major challenge to set folder exclusive access to certain users when shared media is accessible to all. Thus, this study proposed a method to lock a specific shared folder that can only be accessed by utilizing a three-level password approach. The proposed method required users to provide textual password at the first level, then employing a color combination picker at the second level and finally utilizing a picture password in third level. The knowledge of the passwords for each level can only be known by exclusive users in order to acquire access to the protected folder. This enhanced method will ensure the access right would only be granted to users with exclusive rights. Consequently, hard to guess password challenge has the added benefit of hindering illicit folder access attempt.**

Keywords—locked folder; user auntentication; textual password; color combination; picture password

I. INTRODUCTION

In today's world without borders way of working, most organizations provide file sharing infrastructure to promote work collaboration among organization members as well as extending access to external stakeholders in cases of cross collaboration between organizations. Due to the COVID-19 pandemic, the practice of sharing files and folders' popularity has grown rapidly among major organizations striving for boundless file sharing and operational continuity. With technology advancement, huge amounts of data can be transferred over wired and wireless network every second and this has created a need for client-server infrastructure to become more adaptive for big-data file transmission. In addition, the acquisition of file sharing storage is getting more cost effective for either internal network storage or cloud computing space implementation.

The main challenge in folder sharing is folder access permission setting for most generic file sharing system. Many organizations and its stake holders face the difficulty of controlling file sharing permission for certain files and folders in the case where they are required to restrict the access to these files and folders only to a few exclusive personnel according to their access policy. Furthermore, sharing files on this large-scale raise concerns on its security because it introduces risks of hacking, malware infection and loss of sensitive information especially the feared ransomware attack. Thus, organizations have a need to impose tight access control on highly sensitive files to avoid malicious activities involving access of said data and files. Some operating systems, specifically Linux-based distro, is already equipped with folder permission or directory permission that might be suitable to control directory access. However, directory permission control only can be set by the server administrator that would require root account access which could increase the server team workload in order to support the safety of the sharing space.

This study proposes a three-level password to access locked shared folder for use in an organization to promote folder permission control through the development of locked folder application that comes equipped with three-level password algorithm. The computer's directory-level application can be used by anyone that has been permitted to access the sharing space without interference in the operating system's root level privileges. This would make it convenient for both the users' side and the backend side personnel to deal with folders' access control. A three-level password protection mechanism which

could be equipped on a computer app would strengthen the widely used plain textual password which has known vulnerabilities against password attempt attacks such as brute-force, rainbow table and dictionary attack.

II. Background Work

Textual passwords have been widely implemented as access protection in computer systems for both standalone and client-server environments which includes document protection, software piracy control, web-based access control and more. Unfortunately, weak passwords used by users are susceptible to password guessing attack. Walling *et al.* [1] remark that weak passwords are commonly chosen to be easy to recall or something that is obviously noticeable to the user such as birthdate, car registration number, pet's name etc. Contrastingly, a strong password that consist of complex combination of alphanumerical and symbols is hard to memorize since it is usually meaningless to the user. It is something to tradeoff for users to either use an easy to remember weak password or enforcing a strong password that would be quite difficult to remember.

Three-level passwords were designed as one of the efforts to overcome the password dilemma where a series of multifactor passwords are used in an authentication process. As exemplified by [2], the simplest example of multifactor passwords implementation is on online credit card or debit card payment system which require users to provide the card's number, expiry date and three (3) digits verification value (CVV) when issuing the payment. Besides alphanumeric data, there are number of multifactor password methods which involve combinations of textual password with graphical password, biometric identity, digital communication devices, and others.

Graphical passwords were introduced by [3] as cited in [4] with the motivation to ease the hassle of remembering passwords. The graphical password scheme requires users to recall a specific graphical object or file to be used as a password to authenticate a valid user. Most graphical password schemes were designed to be compatible with minimum computer hardware specification. More advanced graphical password schemes require investment in a specific hardware to add on to a system such as biometric identity or digital communication devices. In that case, a combination of textual and graphical passwords is the most preferred combination for multifactor passwords method as well as a three-level password scheme.

There are various three-level passwords combination models designed by researchers. For example, the widely popular Completely Automatic Public Turing test to tell Computers and Human Apart or simply CAPTCHA [5] as mentioned in Guerar *et al.* [6] which is implemented in most of textual password login to prevent bot attack on textual password. In [7] method, the user is required to provide a username and pick the correct combination of images to generate a unique number called One Time Password (OTP) to be matched with the password. Another example is [8] where they defined a textual password as level 1 password, CAPTCHA style password as level 2 and Red Green Blue (RGB) as level 3 password where level 3 password was meant to challenge the level 1 password guessing attack. Based on these aforementioned related works, the three-level password was mainly designed to enhance the safety of textual passwords. Unlike files and folders encryption tools such as MS Office Word password encryption, Portable Document Format password encryption, WinRar and WinZip, the textual password for these tools is not protected with multi-factor password security which then exposes these applications to password attempt vulnerabilities. Thus, the proposed method of this study is quite capable to achieve the goal of protecting documents in file sharing space along with benefits such as flexibility, expendability, and user-friendliness.

III. Methodology

The development of the folder lock with three-level password techniques uses rapid application development (RAD) methodology [9] as a framework. This agile project management is a quick project turnaround method which is widely practiced in software development. Fig. 1 shows the phases in RAD that consists of four phases and iteration in the user design phase.

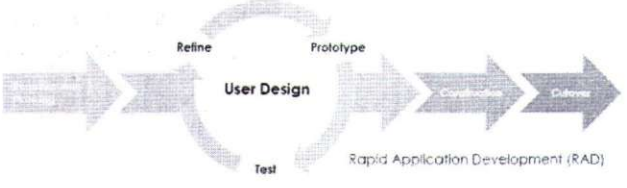

Fig. 1. Phases in Rapid Application Development (RAD)

During the Requirements Planning phase, the potential issues in file sharing in terms of its security and flaws will be identified and that would determine the aim of the study which is to develop a lock folder prototype using the three-level password approach. The aim here is to incorporate a folder level application that is able to lock any specified folder in generic storage with a user defined password. As an addition to that application, the access control mechanism is based on three-level password method as an enhanced protection for the plain textual password which would produce a safer folder lock application.

In the second phase or User Design phase, the lock folder prototype is iteratively designed and developed. The iterative process consists of three major tasks namely refine, prototype and test. In this phase, development commonly begins when the system requirement that was identified in the previous phase is refined to a design feature for prototyping. The user design of lock folder is then developed and built. During the iterative process, the requirement for the locked folder of file sharing is continually refined from the identified requirement, where it was focused only for security in file sharing. A prototype is then developed and tested repetitively to ensure the files inside the locked folder prototype is tamper free. The folder lock prototype is considered as fully compliant in the

user design phase when all of the system test checklist is fulfilled.

Phase 3 is Rapid Construction to transform the initial prototype created during the design phase into a functional model or a working prototype. The phase can be broken down to several steps such as preparing for rapid construction of three-level password techniques and embedding the three-level password techniques into the working prototype.

The last phase, Cutover, is a phase to finalise the locked folder prototype development and testing to ensure the prototype is running well without any errors through a series of findings analysis and statistical analysis. In the future, this study will be focusing more on testing and evaluating the performance of locked folder in terms of its mobility on multiplatform shared storage space and processing resource consumption.

IV. Folder Lock Development

The access to the locked folder using the three-level password mechanism combines three types of access controls: textual password, color combination and picture password. Users are required to register as a valid user prior to logging in to the locked folder. Only then, they may set their first level authentication which is the textual password. In this level, users may set their username and password similar to other common textual access control. Next, in the second level authentication, users are required to set a preferred color combination by combining colors from a color palette, the most common being Red, Green, and Blue. This would serve as the first challenge for previously provided textual password. Finally, the third level password is a picture password, where users are required to select pixel(s) of an image as password points. The procedure of each password level will be replayed during folder lock process and folder unlock process with the same color combination and image pixel points as the enrolled password. The system flow of the proposed method with three-level password techniques is shown in Fig. 2.

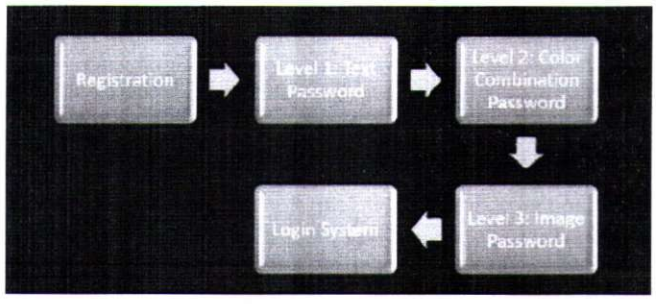

Fig. 2. System flow of locked folder

The textual password or first level password can be any combination of letters, numbers, and symbols on any generic keyboard. This password follows the common practice of building password that should be familiar to the majority of users.

The second level password is color combination that consists of three colors; red, green, and blue (RGB). The RGB trio can be combined to produce a color with three octet eight-bit decimal. For example, (0, 0, 0) is the decimal code for the color black while (255, 255, 255) is the decimal code for the color white. The pseudocode for the second level password or the color combination password (Algorithm 1) is as follows:

```
Algorithm 1: Color Combination Password
Select color: RED, GREEN, BLUE
If first time/reset
    Insert into color values
    Update the color set value
    Record new color combination
Else
    Select the color set value
```

The third level password is picture password where the user must first choose an image in the Joint Photographic Experts Group format (*.jpeg or *.jpg) or the Portable Network Graphics format (*.png). Then, user may set the password by clicking on the image in various locations. When logging in, the user must select the same picture as the password, and then click on the same locations chosen when setting up the password. The third level password or the picture password stage can translate in pseudocode of algorithm 2 as follows:

```
Algorithm 2: Picture Password
Select image (*.jpg/*.png) for password
Set image ratio, height, and width
Convert image to Bitmap
If first time/reset
    Set certain points on the image
    Divide the points into different
    block (create multiple arrays)
    Insert into picture values
    Record selected points
Else
    Select points on the image
```

The practice of implementing a three-level password algorithm consisting of textual password, color combination password and picture password as the password mechanism would make any file sharing space much safer and protected. Consequently, by employing the three-level password mechanism, control to certain folders which may have sensitive or privileged information can be better controlled.

V. Folder Lock Prototype

The folder lock computer application is designed consisted of two pages which are main page, and password page. The main page is illustrated in Fig. 3, which contains three buttons which are the Browse button to open a file explorer, a Lock button to lock targeted folders and an Unlock button to unlock a specified folder. There is also a link to reset a password. A notification status will be shown based on the process invoked by the main button.

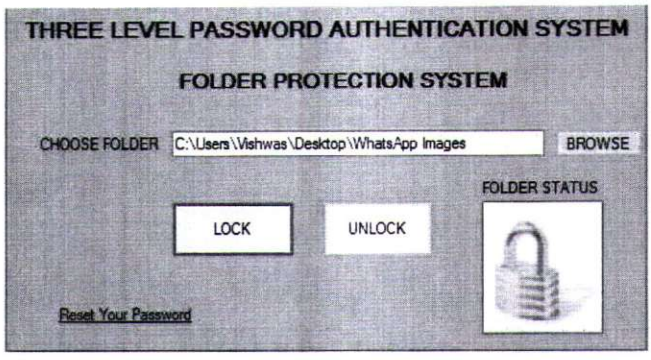

Fig. 3. Main page

Fig. 4 shows the textual password page for Level 1, the textual password. The first prototype for the Level 1 password was limited to four (4) characters to begin with. However, during testing using the brute force attack, the textual password was correctly obtained. Therefore, the Level 1 password requirement was increased to eight (8) characters to increase the time needed for a brute force attack to correctly guess the password.

The page contains a text field requiring users to input their registered username and password to login before being redirected to the next password stage, Level 2

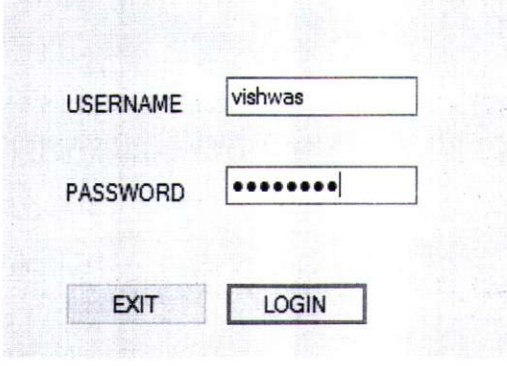

Fig. 4. First level using textual password page

The second level password or the Color combination page displays RGB colors. Users may click any colors to build a Level 2 password based on a color combination (Fig. 5). Users may choose an RGB combination to their favorite color. However, this could be bypassed if the user's favorite color is known to the attacker. Nevertheless, this assumes that the user chooses their favorite color. In the prototype, the choice of colors is limited to only Red, Green and Blue. However, it is worth to note that the RGB color space consists of $256^3 = 16\ 777\ 216$ colors, any of which could be chosen.

Finally, the last or the third level password page is the picture password. User is required to browse and select a picture using Browse button. Then, the user must click at any point (pixel) on the picture as a password as shown in Fig. 6. User may opt to crop the picture for resizing the image (smaller in pixels) and/or changing ration image aspect (length to width).

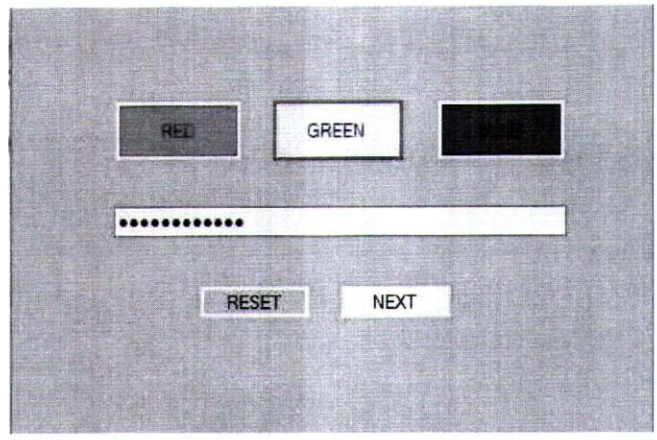

Fig. 5. Second level color combination password

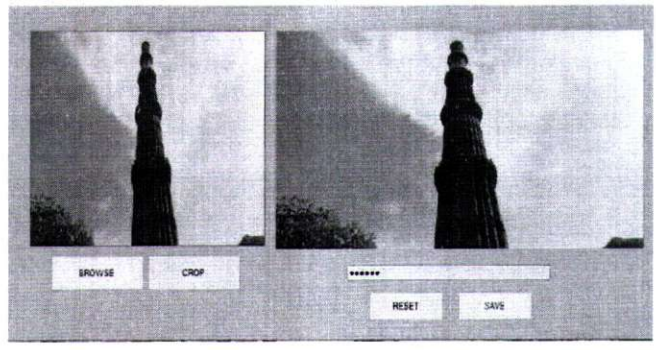

Fig. 6. Third level picture password

VI. DISCUSSSION

This study mainly focuses on the development of a Folder Lock using a three-level password mechanism to control access by users. The initial testing was setup to test the security strength of each password level.

The textual password is evaluated using the brute force method. Initially, the textual password was made up of a combination of four (4) characters comprising of only letters and numbers. However, the brute force attack was able to guess the correct combination quite quickly. Therefore, the textual password requirement is expanded to include symbols, and the number of password character requirement is increased to eight (8) characters. This is important to protect and safeguard all files and data inside the lock folder by making it more difficult for attackers to guess the password combination.

The current color combination technique is limited to only Red, Green, and Blue. In the future, the study will enhance the current prototype by providing more color selection to tighten the locked folder security.

The image password is the most challenging task. The user must meticulously select the exact location (pixels) in order to login to the locked folder. In addition, the bigger the picture the lesser the chance for an attacker to successfully gain access to the locked folder.

As a summary, the benefits of folder lock using a combination of a three-level password is promising. It is able to hinder malicious login attempts into the locked folder. The prototype shows that a three-level password mechanism is able to provide excellent protection of all files in the locked folder. Further research will focus on enhancing the security level of the three-level password mechanism as well as rigorous testing of the folder lock.

ACKNOWLEDGMENT

The authors would like to thank National Defense University of Malaysia for financially supporting the conference paper.

REFERENCES

[1] S. Walling, S. Kielienyu, and S. Lodh, "A Strong Password Generator for user Authentication in Cloud Computing," *Int. J. Eng. Res. Technol.*, vol. 07, no. 12, 2018.

[2] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[3] G. E. Blonder, "U.S. Patent No. 5,559,961," 1996.

[4] Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus, Mohd Nazri Ismail, and Mohd Rizal Mohd Isa, "International Journal of Soft Computing and Engineering," vol. 8, no. 3, pp. 2973–2975, 2019.

[5] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2656, pp. 294–311, 2003.

[6] M. Guerar, L. Verderame, M. Migliardi, F. Palmieri, and A. Merlo, "Gotta CAPTCHA 'Em All: A Survey of 20 Years of the Human-or-computer Dilemma," *ACM Comput. Surv.*, vol. 54, no. 9, Oct. 2021.

[7] A. M, G. S, and A. C.M, "Three Level Security System using Image Based Authentication," *IJARCCE*, vol. 7, no. 11, pp. 133–135, Nov. 2018.

[8] G. S. Mishra, P. K. Mishra, P. Nand, and R. Astya, "User Authentication: A Three Level Password Authentication Mechanism.," *J. Phys. Conf. Ser.*, vol. 1712, no. 1, 2020.

[9] J. Martin, *Rapid application development | WorldCat.org*. Macmillan Pub. Co.; Collier Macmillan Canada; Maxwell Macmillan International, New York, Toronto, New York, , 1991.